AU/ACSC/2014

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

A CYBER FLEET IN BEING

Considering Maritime Strategy as a Basis for Cyber Strategy

by

C. Alan Meadows, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Mike Ivanovsky

Maxwell Air Force Base, Alabama

April 2014

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

ABSTRACT

In order to defend our mission critical systems, we must establish a defense in depth that allows us to observe and defeat threats well beyond the boundaries of our network. The obvious parallels between choke points and lines of communication in the sea and in cyberspace provide a foundation for applying maritime strategies to cyber operations. Following Julian Corbett's theories, a cyber fleet in being is capable of nimbly conducting defensive operations that disrupt and deny the adversary long before he can attack.

"In trying to defend everything, he defended nothing."
- Frederick the Great, King of Prussia

In the internet, we have created something undeniably alluring. The promise of the inexpensive publication of ideas, instant communication between people, businesses and systems, as well as commerce, all unfettered by physical location, have caused a massive rush to bring more and more information onto this common network. In fact, the internet has become the backbone of global economics and communications. But is this wise? Countries and companies alike have joined themselves to this grid, often heedless of the risks it poses, exposing their secrets and vulnerabilities to an inevitable variety of nefarious actors. The game of cyberspace security has always been "breach, then fix," meaning security professionals wait until an actor breaks the security of a system and then implement code to re-secure the breach. The dire implication being that computer systems can never be fully secure and that means information, including our national secrets, will never be secure as long as they exist in the realm of cyberspace.

This is an uncomfortable thought for a country that casually dominates virtually every other aspect of national power. We have long enjoyed a forward projection of power that kept our fights far from home and preserved a sense of total security in garrison. We are not accustomed to operating in contested domains, yet there is no other way to operate in cyberspace. To enjoy the advantages network operations provide to our forces, we must secure our lines of operation. Therefore, operations in cyberspace – particularly defense of military networks - require a new understanding of old ideas. Particularly, certain principles of maritime warfare strategy (such as local control, choke points, and a "fleet in being") may be useful in shaping our ideas regarding contested cyberspace operations. This paper will explore the analogies of sea and cyber warfare and determine where the use of intelligence products may be

helpful in controlling choke points, defending lines of communication and leveraging local control in cyberspace to defend our networks from exploitation, thereby providing freedom of action for our own forces and systems.

A Brief History of the Internet: Vulnerability in your Pocket

What we have come to know as the Internet began as a Defense Advanced Research Projects Agency project in the 1960s. Originally, it was conceived to be a network of networks, connecting civilian research institutions and government agencies via a hub-less topology. The idea was data could travel from one node to any other, even if intermediate legs were unavailable (either for maintenance or in more drastic circumstances, like nuclear attack). The internet remained a little-known, text-based tool, really used only by researchers and academics until the early 1990's when the United States Congress passed legislation authorizing commercial traffic on the network.[1]

Almost immediately, the internet exploded with companies leveraging this new avenue to reach consumers, linking private databases to public web sites. Utility companies saw the opportunity to use public telecommunication lines to connect their subsystems to control stations. The Department of Defense was already using the same telecommunication lines the public internet was on to carry the data for their secret network (SIPRNET).[2] Suddenly, everything was connected. Suddenly, everything was vulnerable.

The internet was designed to ensure communications in the event of a nuclear attack. It was not designed with inherent security capacity. Consequently, defending individual systems or networks is a function of system administrators, which has highly variable degrees of effectiveness. Most system administrators are not as well trained or equipped as the various state actors that have been intruding on government and industry systems for years.

A Brief History of Maritime Warfare Strategies

Julian Corbett wrote his treatise, *Some Principles of Maritime Warfare*, in the opening years of the twentieth century, at a point where naval power had firmly established itself as the first truly global power.[3] His views were actually an extension and adaptation of earlier works on land warfare by Carl von Clausewitz, evolving those elements which lent themselves to the command of the sea. Corbett did not view the sea as something to be controlled simply for the sake of domination because defeating a rival navy did little to end the war in and of itself; rather sea control was a means of controlling commerce and freedom of movement. The definition of control is also different in Corbett's theory of maritime strategy. Instead of seizing and holding a parcel of land, he suggests that being able to decide who transits lines of communication can provide strategic effects that enable victory. By isolating an enemy from commerce, you can literally and figuratively starve them of needed resources.[4] This is the greatest contribution of sea power: providing the pressure that enables other forces to deliver decisive victory.

Specifically, he reasoned the nature of the sea was different than land because it was too vast to be completely controlled and too inhospitable to allow persistent occupation.[5] It is simply impossible to mass enough ships to be a presence in all parts of the sea, so a force must choose either to spread themselves too thin to be effective or mass their ships around areas of importance. The best strategy, he concludes, is to focus on the routes most commonly preferred by ships. These routes can be determined by topology that reduces time spent underway or they may be determined by weather or prevailing winds. Naturally, these features concentrate traffic, both commercial and military, along these lines of communication, reducing the area that needs to be effectively controlled. Certain topological features, like canals or straits, can force traffic along a certain route, creating a "choke point," providing a specific point for a navy to defend or

attack.[6] Exercising local control of choke points is essentially the same as general control of the seas because traffic is tied to the lanes of communication for reasons of efficiency and geography.

Another facet of note in his strategy is the "fleet in being." When a force is numerically inferior to their adversary, seeking to engage them in decisive battle would end predictably. Corbett suggests the best course of action is to adopt a strategy of disruption. A fleet in being is focused on lying in wait in the harbors of their homeland, taking advantage of their enemy while they are in transit and unprepared for attack.[7] By harassing and confounding the enemy's attempt to mobilize or maneuver, an inferior force can prevent their opponent from being able to mass for attack and thereby avoid a decisive action. It is important to note that Corbett does not view this as a strategy that enables victory, but rather simply a way to prolong the conflict on your own terms until a time when more decisive action can be taken.

The Terrain of Cyberspace

As a domain of warfare, cyberspace presents unique challenges to the strategist and operator. First, the domain is not easily understood by laymen. Anyone who has watched a war movie or visited a battlefield can visualize the confrontation of soldiers and how an army moves. It is intuitive in a way that cyberspace cannot be. Very few people have sufficient experience with programming or understand *how* a computer's operating system works, much less how a vulnerability can be found and exploited. Depictions of "hacking" in popular media do not shed much light on the issue, glamorizing the hacker as a shadowy figure who operates alone, motivated by anti-authority sentiments. The actual substance of computer exploits is either not depicted or artificially visualized for the sake of entertainment. The reason for this is simple… modifying computer code is tedious and specific and the skills required to remain at the leading

edge of cyber operations changes daily. For this reason, it is difficult for anyone who is not a cyber-professional to understand what computer network operations actually entail.

The single most confounding difference between warfare in cyberspace and the physical domains,[8] is the munitions, and even the operators themselves, are virtual. This has two implications. First, an attack in the logical network layer does not require the logistical support traditionally associated with physical attack.[9] The weapon is a few lines of computer code released into the network to do their programmed task. It can create mass simply by replicating itself. In certain instances, like STUXNET,[10] the code copied itself over and over; infecting four times as many devices than it ultimately activated itself on, all the while completely erasing any indication of its presence.[11] Attacks like STUXNET can be absolutely silent with no way of discovering their presence unless they are detected entering the system. This is possible because computer systems operate in a virtual world where things can be called into existence or obliterated at will, unlike in the physical world where actions create reactions that must always follow physical laws. It is possible that once a system is compromised, it may be impossible to ever remove the malicious code.[12]

The other implication of operating in a virtual world is that time and distance are meaningless concepts. Data travels along physical network lines at rates approaching the speed of light. Recall that the convenience of the internet resulted in virtually every local network being connected to the global information grid and it is easily understood that literally any system can be reached from anywhere else in the world in mere milliseconds. Now an attacker does not have to concern themselves with the logistical effort of traversing oceans or mountains.[13]

Yet the cyber domain has a physical aspect, doctrinally referred to as the physical network layer.[14] Data travels from node to node on infrastructure, be it fiber-optic cables, copper telephone lines or wirelessly on satellite uplinks or a cellular network. These lines of communication are intuitively analogous to the maritime routes described by Corbett. They represent the paths of least resistance (i.e. most efficient route) for data to travel from one place to another (see Figure 1). Along these routes are ports where packets of data originate and terminate, not unlike sea ports.[15] The physical nature of these ports is significant because they are the only way an attacker can access a given system or network. There is no such thing as "forcible entry" in a network operation because you are limited to the physical connections between the systems.[16] An example of forcible entry in the physical context would be the Marine Corps making an amphibious assault when denied entry to a sea port. Forcible entry in the context of computer network operations does not mean getting past system security by breaking passwords or other action, but rather accessing the target system by a route other than its connection to the internet.

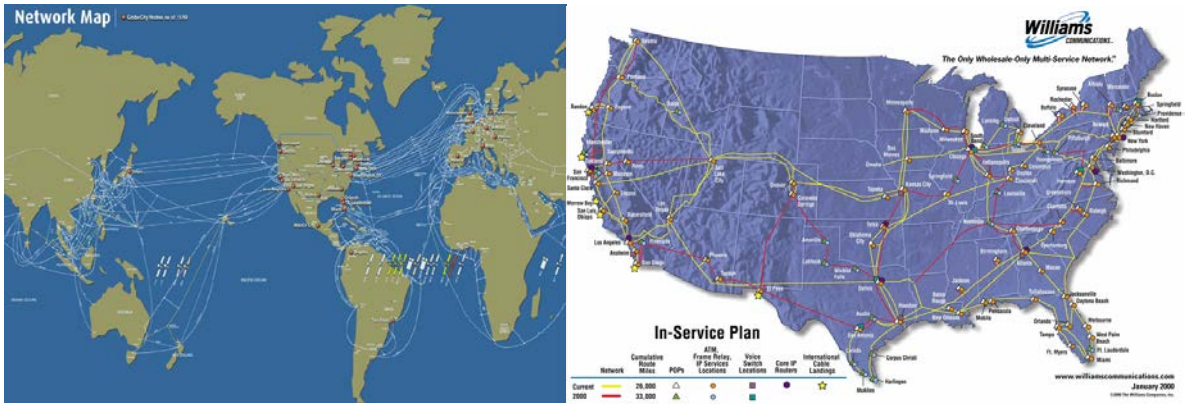

Figure 1. Undersea cables and domestic Internet backbone.[17]

There is one other physical aspect to the terrain of cyberspace: the operator. The end users of computer systems are probably the single largest security risk because they cannot be

programmed to detect, reject and report suspicious behavior. The military has invested significant effort in providing comprehensive, basic Information Assurance and Information Protection training to its users for well over a decade, yet the most significant intrusions on the Department of Defense Information Network (DODIN) have been as a result of poor security discipline on the part of "dumb" users.[18] But even more concerning are the users that work outside the DoD but who handle government secrets as part of their work in the defense industry. These firms conduct research and development for the government, often on classified projects, but the government has limited oversight on how these users are trained to deal with spear phishing or other social engineering attempts. Our adversaries recognize humans as the weakest link in our cyber defense and continually target them in order to gain access to our systems.[19]

Computer Network Defense (CND), the Maritime Way

Given the structure of the seas are echoed so thoroughly in the terrain of cyberspace, it stands to reason some elements of foundational maritime strategy should be of use in cyberspace strategy. In fact, cyber strategy is still in its infancy and the various military services are developing doctrine to define the domain on their own terms.[20] Generally speaking, and without reference to the classified nature of much of this doctrine, cyber strategy fully embraces the idea of computer network defense (CND) that occurs at as great a distance as possible from your own network.

The first principle on which Corbett and cyber strategy agree is the vast majority of cyberspace is essentially neutral territory that cannot be commanded, nor can you expel neutral (or potentially hostile) parties from it.[21] Many neutral parties are commercial interests that provide economic benefits which should be, to some degree, protected. And like the seas, cyberspace traffic neatly aligns itself alone those paths of efficiency we have called lines of

communication. By focusing on these lines, a force is able to bring their capabilities to bear on only those parts of the vast landscape most at risk for exploitation.

We can further refine this effort by focusing on places in the terrain where those lines of communication are most vulnerable to attack, i.e. at the choke points. Whereas choke points in the sea are readily identified by topography (e.g. the Straits of Malacca or the Panama Canal), choke points in cyberspace require more effort to identify and are less physical or permanent which is consistent with the virtual nature of cyberspace. Certainly, based on the risk of human behavior described above, network users are high on the list of a cyber enemy's targets. These individuals may be targeted with social engineering (so called "spear phishing"), wherein an attacker uses false pretenses to get the target to load malicious code on the network. Often, this comes in the form of a disguised link in an email, a website counterfeited to look like a legitimate site, or surreptitiously implanting hidden code on a universal serial bus (USB) drive.[22]

Effective defense of choke points involves many layers, starting with education. The DOD's Information Protection program, which is a form of a defense in depth scheme, educates users on the key aspects of recognizing phishing attempts, but this is just a start.[23] Certain users, though, represent an insider threat because they are intent on either exporting data themselves or enabling a malware exploit that does the same. [24] The task of identifying insider threats in the Air Force falls to the Network Operations Support Center (NOSC), who monitors user actions, especially those exhibiting behavior which breaks user policy or conforms to patterns consistent with data exfiltration.[25] The NOSC operators (known as Cyber Protection Forces in Joint Publication 3-12) rely on an amalgamation of indicators and warnings made available to them via "dashboards." The inputs to these systems range from user validation in the Defense

Enrollment and Eligibility Reporting System to more generic algorithms for suspicious user behavior.[26]

Another choke point in the cyber terrain is the point at which the node connects to the physical network.[27] Since forced entry to a system is not possible at the physical level, any attempt to enter or exploit the system must pass through the node's network attachment point. Systems are often vulnerable at this point because the websites handling authentication have not implemented encryption correctly. An attacker can use such discrepancies to their advantage by "sniffing" the packets passing into and out of the system, decoding the content to reveal login credentials and thus avoiding brute force methods for entry. This is a popular method of exploiting wireless ethernet networks. It has also been a vulnerability in military networks. A computer hobbyist in the United Kingdom discovered he could scan and decode the satellite downlinks from a Predator UAV on a mission in Afghanistan and watch live mission feeds because the data passing between the aircraft and the air operations center (AOC) was not encrypted. There is also evidence Al Qaeda operatives are aware of this vulnerability and used it to thwart some of our operations.[28]

National Protection Teams from USCYBERCOM are tasked to seek out and remediate these vulnerabilities. These so called "Hunter" teams conduct both reconnaissance (blocking) and counter-reconnaissance (tackling) missions.[29] The focus in reconnaissance is to scan friendly networks and systems for vulnerabilities as well as illicit external activity. As vulnerabilities are discovered they are prioritized and remediated. Certain points along the network always present a significant threat, so the Hunter teams maintain a persistent presence, watching for signs of attack. These teams are empowered with broad authority to respond to these attacks. The importance of preapproved engagement authority cannot be understated. Once a system has been

breached, there is potential it will never be fully secured. The Hunter teams also act in a forward capacity, conducting counter-reconnaissance missions against external systems known to provide safe haven to bad actors. We have seen this sort of operation in the civilian world where governments or corporations leverage the legal system to dismantle such sites as The Pirate Bay and MegaUpload, both of which were host to a number of files infected with network exploits.[30]

Apart from defending the well-travelled choke points, cyber forces can use another facet of maritime strategy to conduct defensive operations. The fleet in being is a tactic recommended for a naval force outnumbered by the enemy. Given the broad array of national actors, hacktivists and individual actors that barrage the DODIN every day, there can be little argument that those who defend our network are outmanned. The remedy for this is to move the defense away from the immediate point of entry to the most critical systems (e.g. the AOC, Joint Space Operations Center and Tanker Airlift Control Center) and core systems (e.g. AF Portal, myPay, etc.) to the boundary of the DODIN.[31]

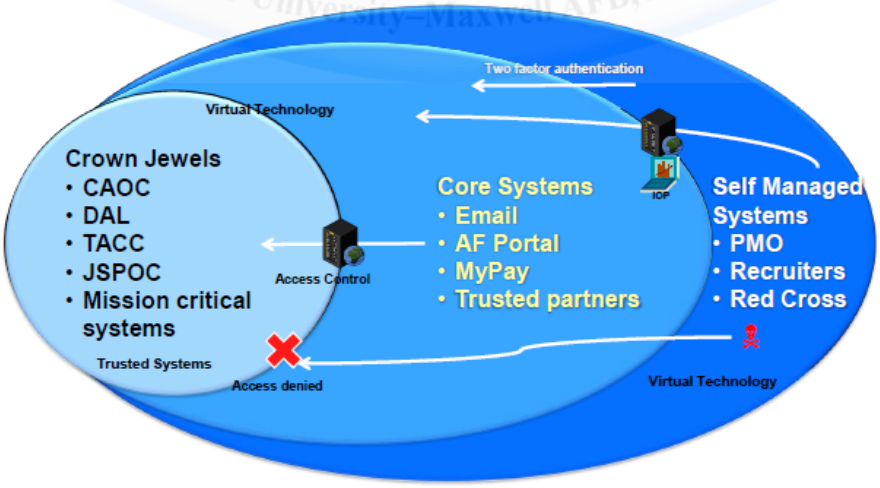

Figure 2. Secure enclaves in the DODIN[32]

The approach described here is a variation on traditional concept of defense in depth. To illustrate, consider the example of a medieval castle.[33] The castle defenses begin with the walls

and then continue inward in successive compartments to make it more difficult to reach the castle's keep. Alternatively, the depth of defense provided by a fleet in being would begin beyond the walls, taking advantage of natural features to funnel and confound the enemy and maximizing the opportunity to defeat them before they reach the castle. The advantage of creating a defense in depth scheme for cyberspace is twofold. First, it establishes successive levels of barriers between an attacker and our most sacred systems. By engaging adversaries outside our system, we can confound their operations and prevent them from massing more attacks, much in the way a small naval fleet can sabotage or disrupt adversary fleets in order to delay decisive action until a more favorable time.[34] Secondly, we can use tactics like counter-reconnaissance missions to disrupt enemy havens or leverage other means to exert economic or informational pressure on adversaries and seize the initiative before their forces are mobilized.[35] In cyberspace, however, attacks happen in milliseconds instead of hours or days, so counter-reconnaissance disruption must be an ongoing effort of a force specifically designed to operate beyond the boundaries of the DODIN.

The extent to which military forces can engage in defensive activities is constrained by US law and doctrine. Joint Publication 3-12 describes the Cyber Attack Response Framework whose guiding principle is proportionality. The commander must first determine the depth and severity of a threat and then choose a proportional response. Depending on the extent of the threat, the response may be as benign as simply observing the attack and collecting intelligence on the operation, not giving away our knowledge of the activity. Or cyber teams may act on a continuum of responses to include denying attacker access to their objective, imposing costs and repercussions for conducting the attack or destroying their capability to attack in the future.[36]

As mentioned previously, a fleet in being is not in itself a path to victory. It merely delays significant action until a more favorable time. Defensive cyber operations are similarly constrained. Because an enemy can cheaply develop and deploy a cyber attack, like a botnet or a distributed denial of service (DDOS), defensive operations will never prevent future attacks. Nor will a defensive posture ever exhaust the enemy of his capacity or will to attack and culminate his offensive. Defense, especially of critical nodes and systems, is crucial because once a system is breached, system administrators must always assume that it is and will always be contaminated because the malicious code is capable of replicating itself and destroying all traces of its presence.[37] A passive defense is not well suited for the cyber realm because software is always vulnerable, and if an enemy is given sufficient opportunity to batter against your defenses, there is a high degree of likelihood they will gain access. Therein lays the value of the active defense strategy described above.

Doing the Right Things or Doing Things Right

There is a difference between efficiency and effectiveness that, though subtle, can be the difference between success and failure in any endeavor. In the case of the former, one is measuring how well a prescribed task was accomplished whereas the latter measure is ensuring the best task was assigned. Measures of effectiveness and performance are already part of the military planning process and they have a place in CNO as well because it is very possible in cyberspace to be doing the wrong task, but doing it very well. As mentioned above, any network can be compromised if attackers are given access to its defenses. If your only measure of network security is the sensing of attacks on your system, then defeat of your network is imminent. Therefore any concept of defensive cyber operations that focuses strictly on network defense will eventually prove itself to be ineffective, even if well executed.

A more apt mindset for defensive operations is that of mission assurance.[38] Rather than focusing on detecting and deterring attacks as they happen, forces should focus on sensing threats far from the home network, in the same way a fleet in being would interdict opposing warships while underway. As an example, Microsoft has an installed base of more than one billion copies of the Windows operating system on computers literally all over the world.[39] Every time one of those computers experiences a program failure, it sends an anonymous report to Microsoft headquarters which is then analyzed to see if the failure was part of a malicious attack or some other cause.[40] Microsoft, therefore, has more than one billion sensors probing cyberspace for threats. These sensors do more for security of Microsoft's network than any firewall could, meaning that instead of crippling their corporate network with filters, firewalls, white-list proxies, or restrictive user policies, they have leveraged their considerable capability to create a safe working space by detecting threats well beyond its boundary. What they understand is that protecting the network is not the objective. Defending the crown jewels is. DCO is not about preventing attacks on the physical or logical layers of DODIN… it is about defending our critical mission systems from being altered or damaged, assuring the mission of flying and fighting can continue unabated.

The Importance of ISR to DCO

Because of the speed at which operations in cyberspace take place, developing a system to deliver consistent and accurate situational awareness is critical. This is the role of cyber intelligence, surveillance and reconnaissance (Cyber ISR). Analysts can provide specific intelligence preparations of the battlefield (Cyber IPB) that detail the nature of the threat (symmetric or asymmetric; national or individual), key terrain (network topology, defense mechanism, tactics) and likely enemy courses of action. Network surveillance operations, human

intelligence and signals intelligence all contribute to this portfolio of data cyber operators rely on to make informed decisions during their time-sensitive operations. These tools also help operators recognize and identify trends and patterns of behavior that are useful in denying the adversary their objective.[41]

Cyber ISR also acts as a focal point for forensic analysis. Identifying the source of an attack and attributing responsibility is an extremely difficult and important task. Many attacks are carried out under a "false flag," meaning the originator of the attack has purposefully designed elements of an operation to suggest it was carried out by some entity other than his organization. For example, a hacker in North Korea might include language cues, use network routing, or employ tactics suggesting the attack was conducted by a Chinese operator. This is problematic because accurate attribution is a critical part of planning and executing counter strikes or a diplomatic demarche. Intelligence Mission Data like this enables better targeting options and requires intelligence expertise from across the full range of collection.[42]

Conclusion

Technology changes things. It opens doors to new worlds and provides the means by which we explore their knowledge, exploit their resources and execute our will over them. This has always been the way of things, whether it was man's first foray onto the seas, his conquest of the air, or his reach into space. Being creatures of habit, we have often learned through difficulty that the unique character of each domain requires a reexamination of previously held beliefs about how best to subjugate it. Old lessons must be revised or even discarded in order to develop strategies that best complement the character of the new domain. Now, we have constructed a pervasive network of computers that connects every corner of the globe with unprecedented access to commerce, information and communication. We have simultaneously created the single

biggest vulnerability any government, company or military force could envision: a direct path to the heart of our enterprise that is easily exploited and potentially undetectable.

In order to defend our mission critical systems, we must establish a defense in depth that allows us to observe and defeat threats well beyond the boundaries of our network. The obvious parallels between choke points and lines of communication in the sea and in cyberspace provide a foundation for applying maritime strategies to cyber operations. A cyber fleet in being is capable of nimbly conducting defensive operations that disrupt and deny the adversary long before he can attack.

Bibliography

Air Force ISR 2023: Delivering Decisive Advantage, (Washington DC: Air Force Press, 2013).

David Aucsmith, *A Theory of War in the Cyber Domain*, Microsoft Institute for Advanced Technology in Governments, 5 March 2012.

Dave Barnhart, *Air Force Strategy that Drives our Cyber Acquisition*, 24th Air Force/CG, slides.

Joel Brenner, America the Vulnerable (New York: Penguin Press, 2011).

Mike Bordick, *AF Cyber Superiority Architecture*, Headquarters Air Force Space Command/A6I, slides.

Richard Clarke, *Cyber War* (New York: Harper & Collins, 2010).

Julian Corbett, *Principles of Maritime Strategy* (Mineola, New York: Dover Publications, 2004).

Joseph Elbaum, "Cyber Power in the 21st Century," Research Report (Wright-Patterson AFB, OH: Air University, 2008).

Enterprise Service Desk (ESD) Operating Concept, Air Force Space Command document, 5 February 2013.

Kamal Jabbour, Ph.D. and Muccio, Sarah , Ph.D.. "The Science of Mission Assurance." *Journal of Strategic Security* 4, no. 2 (2011): 61-74.

Joint Publication (JP) 3-12. *Cyberspace Operations*, 11 Feb 2013.

Martin Libicki, *Crisis and Escalation in Cyberspace*, (Santa Monica, CA: RAND Press, 2012), 144.

Operating Concept for Cyberspace Security and Control System (CSCS), Air Force Space Command document, 23 September 2012.

Notes

[1] Joel Brenner, America the Vulnerable (New York: Penguin Press, 2011), 33.
[2] To be clear, SIPRNET packets do not interacting with regular internet servers, they are simply transmitted on the same copper wire infrastructure as internet packets.
[3] ACSC, AP.
[4] Julian Corbett, *Principles of Maritime Strategy* (Mineola, New York: Dover Publications, 2004), 99.
[5] Corbett, 89.
[6] Corbett, 132, 161.
[7] Corbett, 176.
[8] Technically, and according to Joint Publication 3-12, cyberspace is a physical domain (computers, wires, chips, etc) with a virtual component. This distinction is more relevant when discussing exploits or attacks with kinetic consequences than when trying to characterize the domain as a whole.
[9] JP 3-12, 13.
[10] STUXNET is a malware program designed to infiltrate the control systems of nuclear power plants and was identified as the cause of several mishaps within the Iranian nuclear research program.
[11] Brenner, 102.
[12] Brenner, 45. In 2010, Google recused itself from operating in China. Publicly this change was about the Chinese government's requirement that search results be censored and filtered to support the party line. In reality, Chinese hackers had so thoroughly infiltrated Google's system that there is lingering suspicion that a back door has been installed in their corporate network.
[13] Joseph Elbaum, "Cyber Power in the 21st Century," Research Report (Wright-Patterson AFB, OH: Air University, 2008), 70.
[14] JP 3-12, 13.
[15] Martin Libicki, *Crisis and Escalation in Cyberspace*, (Santa Monica, CA: RAND Press, 2012), 144.
[16] ACSC, AP.
[17] Elbaum, 71, 75.
[18] Brenner, 82.
[19] Brenner, 63.
[20] This paper will only address the US military's role in cyberspace and the defense of the DODIN. There are, of course, titular authorities that define the areas of responsibility for defense of the .gov network. These artificial boundaries are known limitations to the effectiveness of cyber defense forces, though there is currently no expected change to the US Code to alleviate the situation. Particularly alarming is that there is no real oversight of the commercial internet. Companies are left on their own to secure their data. History has shown, however, that companies either do not take this responsibility seriously or are unable to for either technical or economic reasons. This presents an enormous risk to the DODIN and other government secrets because so much research and development is done by industry. For a more complete discussion, see Joel Brenner's *America the Vulnerable.*
[21] Corbett, 89.
[22] Operating Concept for Cyberspace Security and Control System (CSCS), Air Force Space Command document, 23 September 2012, 3.
[23] Cyberspace Security Control Systems, 10.
[24] Cyberspace Security Control Systems, 3.
[25] Cyberspace Security Control Systems, 10.
[26] Mike Bordick, *AF Cyber Superiority Architecture*, Headquarters Air Force Space Command/A6I, slides.
[27] David Aucsmith, *A Theory of War in the Cyber Domain*, Microsoft Institute for Advanced Technology in Governments, 5 March 2012, 3.
[28] Brenner, 89.
[29] Dave Barnhart, *Air Force Strategy that Drives our Cyber Acquisition*, 24th Air Force/CG, slides.
[30] Bordick slides.
[31] Bordick slides.
[32] Bordick slides.
[33] ACSC, AP.
[34] Aucsmith, 11.

Notes

[35] Corbett, 176.
[36] JP 3-12, *Cyberspace Operations*, 5 Feb 2013, 15.
[37] Elbaum, 71.
[38] Jabbour, Kamal , Ph.D. and Muccio, Sarah , Ph.D.. "The Science of Mission Assurance." *Journal of Strategic Security* 4, no. 2 (2011), 62.
[39] Personal interview with AF/ST.
[40] The analysis focuses on the intent of the code that was running. To a processor, computer instructions from a virus are the same as the instructions for a word processor. It requires trained security personnel to be able to classify a bit of code as malicious or benign. This process is obviously slow (in machine time) which is another reason why waiting to detect intruders until they are on your network is a losing proposition. NB: 30% of software crashes are attributed to malicious intent.
[41] Enterprise Service Desk (ESD) Operating Concept, Air Force Space Command document, 5 February 2013, 31.
[42] *Air Force ISR 2023: Delivering Decisive Advantage*, (Washington DC: Air Force Press, 2013), 5.